Abstract

This invention provides an improved mechanism to guard against message sequencing threats. It can be used in any system which makes use of a transform which uses a state machine such as encryption/decryption and compression/decompression systems, and where the transform and the inverse transform use the same state machines. The invention is implemented as a matching pair of applications at both ends of a transmission link. The transmitting end encodes the current value of a particular state using a one-way hash function and adds this value as a field in the transmitted packet. At the receiving end, the packet is passed to the decoding algorithm which derives the current value of the same state, and passes it through the same one way hash function. The receiver can compare the result of these operations with the value in the field sent by the transmitting end.